Gain flexibility to data access options with Combination taps

Changes in network infrastructure media-type, increases in utilization, and evolving analysis solution requirements call for an increase in the flexibility and configurability of network tapping solutions. This white paper will show how the enhanced features and manageability of the newest generation of Combination taps from Fluke Networks can provide the flexibility, cost efficiency and sophistication for network test, measurement and security solution deployment that will help to meet these challenges.

Table of contents

FLUKE networks

Introduction

The deployment of network taps, multi-port link aggregators and link regenerators is rapidly becoming a de facto standard for data access in today's networks. These devices replace mirror or SPAN ports, providing data access for devices performing security monitoring, data collection, application and protocol analysis, web usage monitoring and a wealth of other activities.

The rationale for deploying such an increasingly broad range of test, measurement and security solutions is driven by many factors – among them the need for faster mean time to resolution (MTTR) on mission-critical networks and requirements for adherence to a wide variety of compliance regulations including CALEA, Sarbanes-Oxley and others.

The types of taps, aggregators and regenerators selected and deployed for particular projects are dictated by many factors. These include the specific number of inputs and outputs required, media-type of the monitor cards on the analysis devices and the speed or type of link being tapped. When long-term projects evolve or network visibility requirements change, such devices may not be adaptable to a wider variety of uses, thereby limiting flexibility or requiring costly acquisition of new analysis solutions.

Changes in network infrastructure media-type, increases in utilization, and evolving analysis solution requirements call for an increase in the flexibility and configurability of network tapping solutions. This white paper will show how the enhanced features and manageability of the newest generation of Combination taps from Fluke Networks can provide the flexibility, cost efficiency and sophistication for network test, measurement and security solution deployment that will help to meet these challenges.

The network: accessing data for test, measurement and security

Network access for data analysis has experienced an exponential increase in complexity since the era of early-shared media environments. The simplicity of attaching a monitoring or data capture solution to a shared media Ethernet hub or a Token Ring MAU was replaced in the mid-1990s by the challenge of gaining visibility into switched networks.

As networks grew in complexity, the device manufacturers began offering mirror/SPAN ports that enabled directing copies of data to a dedicated monitoring port and the attached analysis solution. Over a period of years, the sophistication of such ports increased – moving initially from only allowing visibility into unidirectional traffic on a single port to eventually offering the option to look at bidirectional traffic on a single port, group of ports or even a VLAN.

Despite these advances, mirror/SPAN ports still have a number of shortcomings and issues of concern:

- Configuring a SPAN session "on the fly" puts a busy network at risk.
- Possible performance impact on the switch itself when a SPAN session is initiated.
- The potential for oversubscription of the SPAN port and the limited number of available ports.

Taps and aggregators: an alternative means of data access for test, measurement and security

The development of network taps has allowed passive in-line access to specific physical links – eliminating concerns about misconfigured SPAN ports or the impact on switch performance. Multi-port aggregators, which merge data provided from multiple links, SPAN ports or a combination of the two, and regenerate a number of copies, provide a useful means of allowing a single analysis solution to view data from multiple links or points of interest on the network.

Full-duplex taps, which hand off separate copies of the Rx (inbound) and Tx (outbound) data from a tapped link, have evolved with the addition of aggregation taps – a design that internally combines the Rx and Tx data copies before handing it off to the data analysis solution. Multi-port aggregators have also evolved to include regeneration – a function that takes one or two inputs and creates a larger number of identical copies.

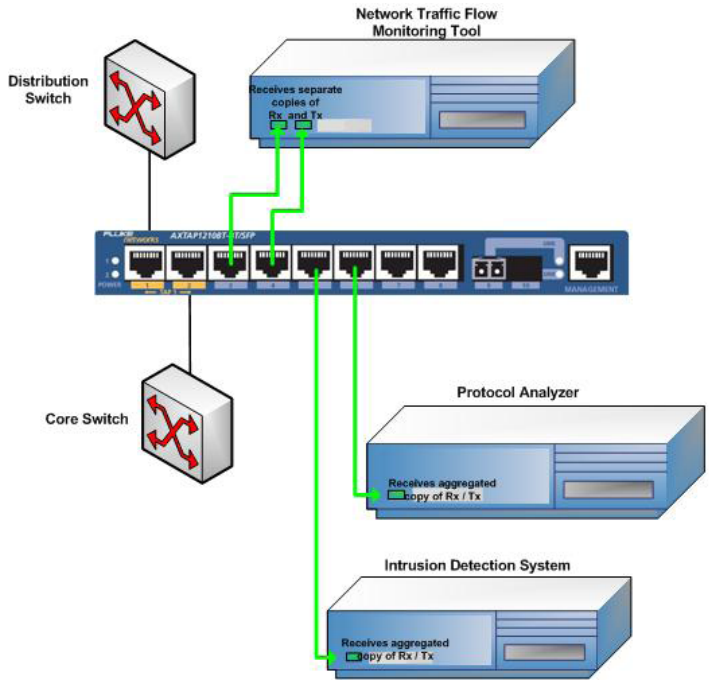
All three categories include, in most cases, the option to media convert the output – e.g. a fiber link or input can be converted for a solution with a copper monitor interface, or data from copper sources can be provided as fiber to solutions with that media-type interface.

Monitoring bidirectional network traffic: balancing the needs of different analysis solutions

The vast majority of network analysis solutions, including most protocol analyzers and intrusion detection systems, support only a single interface card for data capture and analysis. Traditional full-duplex taps, despite the many advantages they provide relative to mirror/SPAN ports, do not allow the user to simultaneously capture and view both sides of a duplex conversation unless the analysis solution has dual interface cards that can be synchronized.

Aggregation taps, which combine copies of the Rx (inbound) and Tx (outbound) traffic on a link, have provided a solution to this challenge. A new generation of products is appearing that provides statistical analysis of traffic based on bidirectional conversation flow. Separate copies of Rx and Tx are required for the multiple monitor cards in such devices, but this presents a conflict with the needs of existing solutions that have a single interface and require aggregated copies of Rx and Tx data.

Figure 1A

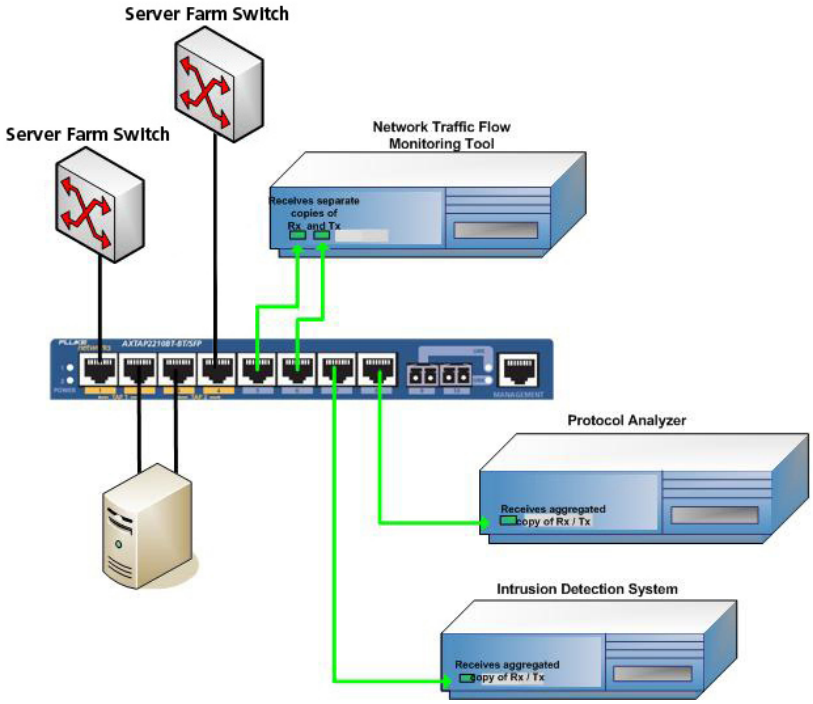


In Figure 1A, the Combination tap hands off separate copies of the Rx and Tx traffic to an analysis device measuring bidirectional traffic flow. The protocol analyzer and IDS receive aggregated copies since these solutions support only a single interface and do not need separate Rx and Tx copies.

The contrasting needs of these different solutions present a dilemma that cannot be resolved with mirror/SPAN ports or conventional aggregation taps – how to view both aggregated and non-aggregated versions of the identical data from a single tapped link or dual tapped links.

Combination taps provide a simple solution to this vexing problem. The devices pictured can tap either a single link or dual links. They may be configured for the copies of Rx and Tx traffic on the link to be aggregated out any port or sent out as separate non-aggregated data streams. The data may also be regenerated multiple times to different solutions based on user preference.

Figure 1B



The dual link Combination tap in Figure 1B allows multiple Rx and Tx data copies to be aggregated together out different ports if desired. In this example, the Rx of both tapped links is handed off from one monitor port and the aggregated Tx copies form a different port. In this particular instance, the overall utilization was low, allowing all traffic from both links to be aggregated.

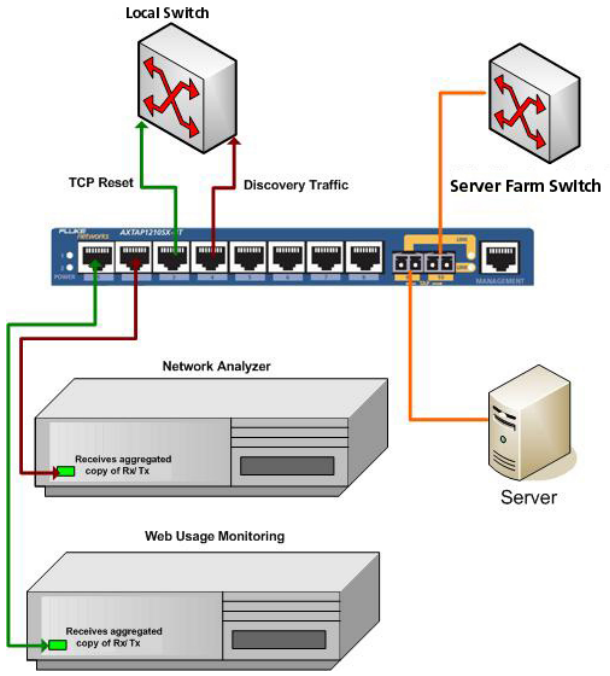
Traffic injection: discovery process and TCP reset on fiber links with single NIC

A number of network analysis and monitoring solutions offer valuable features that require a single interface to send traffic onto the network, as well as receive data for analysis. For example, a network analyzer may be able build a Visio map of the local subnet based on traffic seen on the tapped link, or a Web usage-monitoring device can terminate a session with a "TCP reset" and send an ICMP unreachable message to the offending user.

This functionality is not possible with many mirror/SPAN ports – which disallow ingress traffic – although it has long been possible via copper taps that have bi-directional traffic enabled. Fiber links are tapped via an optical splitter whose directional characteristics make it impossible to send traffic back onto the tapped link directly from the monitor card through the tap.

Combination taps provide an elegant solution to this challenge by allowing any traffic leaving the monitor card to be handed off from a single monitor port of the tap to a local switch. Ingress traffic on that monitor port can be disabled – thus providing a secure solution that enables the desired functionality but leaves the monitoring solution invisible to the network – as prudent security practices dictate.

Figure 2



As link utilization increases, Combination tap reconfiguration from aggregation to full-duplex mode accommodates full line rate analysis.

Link utilization increases: adapting taps to accommodate network traffic growth

Historical trends have shown that network link utilization, despite ongoing topology speed increases, continues to rise. The addition of more users, more servers and adoption of more bandwidth-intensive applications are among the factors contributing to this trend.

Aggregation taps, which combine copies of the Rx (inbound) and Tx (outbound) traffic on a link, have long presented an acceptable solution for monitoring full-duplex links with existing solutions that have a single NIC and require an aggregated copy of Rx and Tx.

As an increasing number of network test, measurement and security solutions offer the option of multiple analysis interface cards on a single chassis and full-duplex links begin routinely exceeding an average of more than 50% utilization, the aggregation tap may begin experiencing packet loss of the copied Rx and Tx data and no longer be a workable solution.

Combination taps provide an upgrade path in several ways – all achieved by reconfiguring the tap functionality to match link utilization, rather than investing in new taps. In Figure 3A, all of the attached analysis solutions receive aggregated copies of the Rx and Tx data. In Figure 3B, the same tap has been reconfigured to accommodate higher utilization levels by placing additional monitor card capacity on the analysis devices and using the tap in non-aggregated mode to hand-off separate non-aggregated copies of Rx and Tx data.

Matching data needs to analysis solutions: accommodating changing media support

The growing number of analysis solutions being deployed on the network and the varying requirements of the groups who need network data access has created contention for access to SPAN ports. This challenge has driven the development of taps with multiple identical outputs and of multi-port regenerators that can replicate the data coming from existing taps or from SPAN ports.

Figure 3A – "Before"

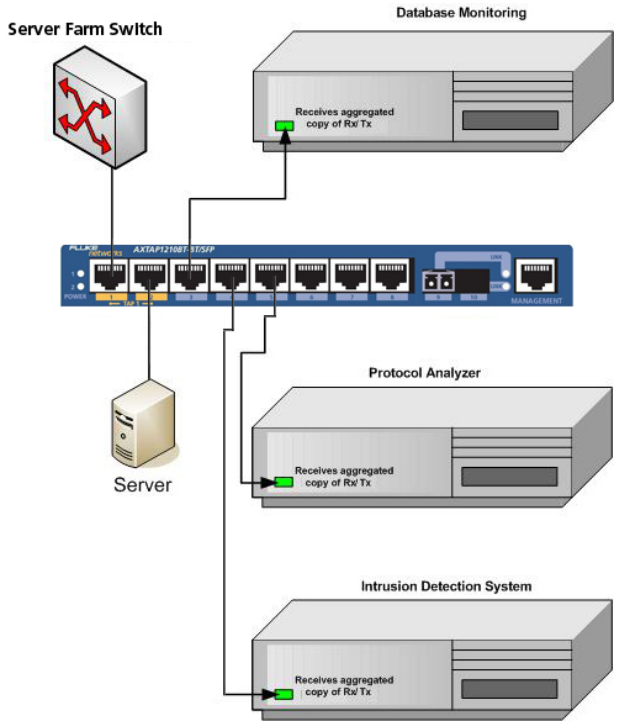
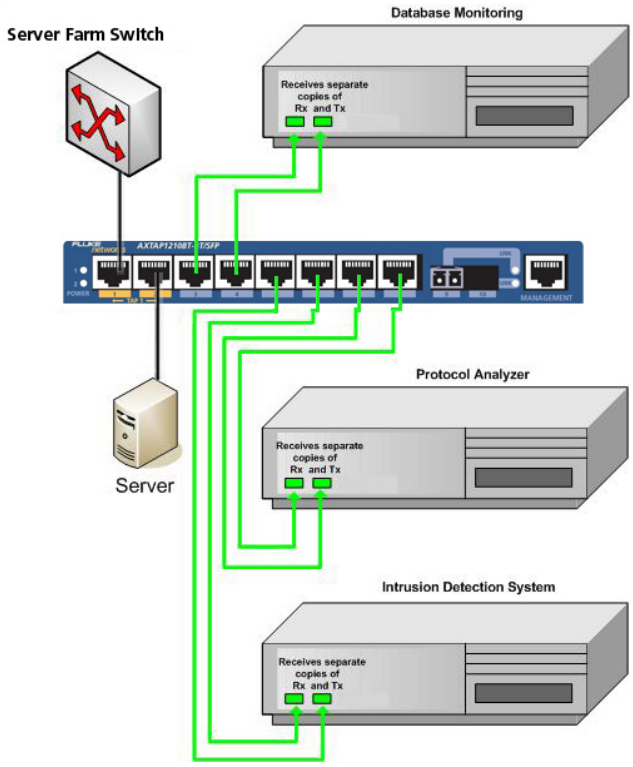


Figure 3A – "After"



These solutions have been effective but have limitations of their own. Such devices come built to a specific configuration with pre-determined inputs, monitor ports, and fixed media types.

Combination taps have specific ports dedicated to serve only as in-line tap ports, with the remaining ports configurable as input ports or as monitor ports. Additional flexibility is gained through two SFP (small form pluggable) receptacles on each Combination tap – which allow those two ports to be used as either fiber or copper media.

Summary

Network data access is a growing requirement for IT groups that rely on test, measurement and security solutions for greater network performance and uptime. As with all technology equipment decisions, procurement of flexible solutions always helps hedge against the inevitable change that accompanies almost all network systems and architectures. The 1210 and 2210 series Combination taps from Fluke Networks support the growing need for data access, while also providing configuration options that minimize the risk associated with change. When evaluating the deployment of new network access points on your network, keep in mind the need to move from aggregated data flows to full-duplex data. In addition, proliferation of analysis devices will inevitably require a greater number of replication ports, which is a simple configuration away on these devices.

About Fluke Networks

Fluke Networks is a leading provider of network and application performance management solutions. The company's technologies enable enterprises to reliably and securely manage the delivery of mission-critical applications across their infrastructure. Fluke Networks' products increase application and network availability, optimize the use of bandwidth, and reduce operating costs across traditional and IP-based infrastructures. For more information on our complete selection of Tap and Switch solutions visit **www.flukenetworks.com/taps.**